Priority of Critical Infrastructures
(based on Region 6 survey information)

The Strategic Plan should address the protection of the critical infrastructures in Region 6. Fifty-one stakeholders in Region 6 were asked to rank the top five priorities from a list of critical infrastructures. The following table summarizes the data on prioritized critical assets and infrastructures to protect. In their responses, the stakeholders considered both the vulnerability of the critical infrastructure and the potential consequences of disrupting the infrastructure. Note that many mentioned the importance of protecting the port (e.g., port as conduit of food, hazmat, and transportation) even though it was not specifically identified as a critical infrastructure category. There was also an overall deep concern about interdependent infrastructures, but this result is not easily reflected in the table of prioritized infrastructures. The stakeholders listed the critical infrastructures in order of concern. In tabulating the data, we included the first 3 or so critical infrastructures as top concerns and the next two or more as medium concerns. We conclude that the top critical infrastructures mentioned were energy, transportation, and water. The medium concerns were public health, emergency services, and information and telecommunications.

Critical Infrastructures to Prioritize	Top Concern	Medium Concern	Total
Agriculture and Food	4	2	6
Banking and Finance	2	6	8
Chemical Industry/HAZMAT	1	4	5
Defense Industrial Base	3	0	3
Emergency Services	9	1	10
Energy	19	5	24
Government Facilities/Agencies	4	4	8
Information and Telecommunications	5	6	11
Law Enforcement	5	4	9

Critical Infrastructures to Prioritize	Top Concern	Medium Concern	Total
National Monuments and Icons	2	0	2
Postal and Shipping	2	1	3
Public Health	8	6	14
Transportation	13	9	22
Water	16	4	20
Ports (not originally listed as choice)	5	1	6
Other	1	0	1

Needs of Infrastructure

The following are the specific needs identified by Region 6 stakeholders in protecting critical infrastructures. This is followed by possible strategies to meet the need (developed from either the stakeholders or from input from ICF).

Need 1. Identify CIP: There is a great need to assess which infrastructures are critical in Region 6 and to determine how best to protect them. This need was the most frequently identified need.
Possible Strategy to Meet Need: Ask Region 6 stakeholders to identify priority critical infrastructures (see above). Examine/analyze jurisdiction/state data from Statewide Needs Assessment and Three Year Strategy. Using GIS, map infrastructures to help with identifying critical ones and interdependencies as well as determining best methods for protection. Hire outside party/consultant to conduct analyses.

Need 2. Develop CIP Plan: Develop specific Critical Infrastructure Protection Plans. This need was also widely held.
Possible Strategy to Meet Need: In secure forums, government should meet with leaders of critical infrastructures to share concerns, capabilities, and possible ways to coordinate/share plans. Determine how to develop plans.

Need 3. Develop COG/S: Develop and exercise Continuity of Government and Services (COG/S) plans as jurisdictions and as Region 6. This was mentioned multiple times. For example, backup operations were needed such as 911 system backup, EOC backups, and alternative energy backup generators. Additionally, building security is mentioned.
Possible Strategy to Meet Need: Facilitated effort at training on importance of COG/S for executives and training for program staff. Identify preliminary issues, and work out solutions with key stakeholders. Follow new FEMA guidance for State/Locals on

Developing COOP/COG plans. Develop facilitate regional exercise focusing on COG/S. Obtain federal grants to fund specific backup equipment.

Need 4. Harden CI: Harden critical infrastructures. For example, older transportation and building infrastructures are not robust for handling earthquakes/explosion danger. Another example is wellhead protection.
Possible Strategy to Meet Need: This can be very expensive to retrofit buildings, bridges, etc. Also, development time is lengthy. Perhaps need to prioritize: perform consequence/vulnerability analysis of specific infrastructures and perform cost/benefit analysis. Some protection is mandated through ordinances (e.g., wellhead protection).

Need 5. Improve Hospital/Public Health Infrastructure: Some sense that hospital system preparedness varies in preparedness/robustness. Many feel public health is weak link particularly with bioterrorism.
Possible Strategy to Meet Need: Obtain Health Resources and Services Administration Cooperative Agreement for Bioterrorism Hospital Preparedness (HRSA) grants to perform assessment of hospital preparedness. Region 6 strategies may focus on interrelationships and coordination of hospitals.

Need 6. Deterrence/Surveillance: More deterrence of terrorism/crimes against critical infrastructure protection. Region 6 needs more quick response from trained personnel (e.g., law enforcement) and coordination of enforcement from other jurisdictions to protect critical infrastructures. Need more surveillance equipment (e.g., cameras) and barriers (e.g., fencing). All these assets supplement private security of CIP when there are general or specific threats against critical infrastructure sectors (e.g., U.S. DHS gets general threat against ports, asks for local/regional support for creating security buffer/surveillance around port for a week). This need was mentioned quite a few times.
Possible Strategy to Meet Need: More funding for training and equipment.

Need 7. Secure Information: Lack cyber protection and staff expertise to provide such protection.
Possible Strategy to Meet Need: Share capabilities (e.g., inexpensive fixes, guidance) of those prepared jurisdictions with those that need protection.

Need 8. Coordinate with CI: More coordination with private sector that own critical infrastructure. Specifically, need safe forum to talk/share sensitive information.
Possible Strategy to Meet Need: Explore use of ISAC where created. Review and change public disclosure laws. Develop protocols and have physical equipment for security communication and sharing.